08-435-M-01

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

1. Your affiant in this matter, Donya Jackson, has been a Special Agent with the Office of the Inspector General at the Library of Congress since May 2007. Prior to her employment with the Library of Congress, your affiant was a Special Agent with the United States Secret Service since 2000. During your affiant's six year tenure with the U.S. Secret Service, she was assigned to the Criminal Investigation Division in Headquarters, and the New York Electronic Crimes Task Force based out of the New York Field Office, Brooklyn, New York. Your affiant has received training in the following subject areas: Basic Investigator Course, Interview and Interrogation, Undercover Computer Investigation Techniques, SEARCH High Tech Crimes Investigations of Computer Crimes Course, Investigation of Online Child Exploitation Course, and Search and Seizure of Electronic Evidence Techniques. Your affiant has made numerous arrests and interviewed numerous victims, witnesses, and suspects.

2. Your affiant has participated in numerous online investigations, and undercover online investigations.

3. This affidavit is made in support of an application for a warrant pursuant to 18 U.S.C. § 2703(a) and § 2703(b)(1)(A) to compel Microsoft Corporation, a provider of electronic communication and remote computing services,1065 La Avenida, Mountain View, CA 94043 to provide subscriber information, records, and the contents of wire and electronic communications pertaining to the account [redacted]. The records and other information requested are set forth in Attachment A. There is probable cause to believe that the contents of the wire and electronic communications pertaining to the subject accounts are evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. § 1028 (Fraud and Related Activity in

Connection with Identification Documents, Authentication Features, and Information). *See* 18 U.S.C. §§ 1028(a)(2), 1028(a)(7)("Whoever ... (2) knowingly possesses with intent to use unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents; [and] (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit .... any unlawful activity ... shall be punished [under] this section.")

Facts and Circumstances

4. The statements in this affidavit are based on my personal investigation and on information provided by other law enforcement agents including Special Agent Pamela Hawe, of the Library of Congress Office of the Inspector General and on my experience and background as a Special Agent. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

5. In my training and experience, I have learned that Microsoft Corporation ("MICROSOFT") is a company that provides free web-based Internet electronic mail ("e-mail") access to the general public, and that stored electronic communications, including opened and unopened e-mail for MICROSOFT subscribers may be located on the computers of MICROSOFT. Further, I am aware that computers located at MICROSOFT contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seek authorization to seize the records and information specified in Attachment A.

Search Procedure

6. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization to permit employees of MICROSOFT to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to MICROSOFT personnel who will be directed to isolate those accounts and files described in Section II of Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, MICROSOFT employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A, including an exact duplicate of all information stored in the computer accounts and files described in Section II of Attachment A;

c. MICROSOFT employees will provide the exact duplicate in electronic form of the accounts and files described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

d. Law enforcement personnel will thereafter review all information and records received from MICROSOFT employees to determine the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.

Background Regarding Computers, the Internet, and E-mail

7. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1) and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility

or communications facility directly related to or operating in conjunction with such device.

8. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

c. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

d. IP addresses are conventionally written in the dot-punctuated form *num1.num2.num3.num4* (*e.g.*, 216.109.118.74). There are two types of IP addresses: dynamic and static. A static IP address is one that is permanently assigned to a given computer on a network. With dynamic IP addressing, however, each time a computer establishes an Internet

connection, that computer is assigned a different IP address. For example, each time a Comcast customer with a dynamic IP address connects to the Comcast network and establishes an Internet connection, he or she is randomly assigned an IP address from the block of IP addresses controlled by Comcast. When the customer ends the session, the temporarily assigned IP address is placed back into the pool of IP addresses available for temporary assignment to other Comcast subscribers. Customers using broadband Internet services are typically assigned IP addresses that are technically dynamic, but which may remain unchanged for longer, but not indefinite, periods of time (*e.g.*, one week).

Microsoft Corporation, MSN

9. Based on my training and experience, I have learned the following about MICROSOFT:

a. MICROSOFT, MSN is an e-mail service which is available free of charge to Internet users. Subscribers obtain an account by registering on the Internet with MICROSOFT. MICROSOFT requests subscribers to provide basic information, such as name, gender, zip code and other personal/biographical information. However, MICROSOFT does not verify the information provided;

b. MICROSOFT maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, e-mail transaction information, and account application information;

c. Subscribers to MICROSOFT may access their accounts on servers maintained and/or owned by MICROSOFT from any computer connected to the Internet located anywhere in the world;

d. any e-mail that is sent to a MICROSOFT subscriber is stored in the subscriber's "mail box" on MICROSOFT's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by MICROSOFT. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on MICROSOFT's servers indefinitely;

e. when the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to MICROSOFT's servers, and then transmitted to its end destination. MICROSOFT users have the option of saving a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the MICROSOFT server, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained at MICROSOFT, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations;

f. a MICROSOFT subscriber can store files, including e-mails and image files, on servers maintained and/or owned by MICROSOFT;

g. a subscriber to MICROSOFT may or may not store copies on his/her home computer of e-mails and image files stored in his/her MICROSOFT account. The subscriber may store e-mails and/or other files on the MICROSOFT server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer

in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the MICROSOFT server;

h. as a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of MICROSOFT may not be. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. MICROSOFT employees may not be. It would be inappropriate and impractical, however, for federal agents to search the vast computer network of MICROSOFT for the relevant accounts and then to analyze the contents of those accounts on the premises of MICROSOFT. The impact on MICROSOFT's business would be severe;

i. in order to accomplish the objective of the search warrant with a minimum of interference with the business activities of MICROSOFT, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow MICROSOFT to make a digital copy of the entire contents of the information subject to seizure specified in Section II of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A; and

j. executing a warrant to search a MICROSOFT e-mail account requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject e-mail account in this case for evidence of the target crimes will require that agents cursorily inspect all e-mails produced by MICROSOFT in order to ascertain

which contain evidence of those crimes, just as it is necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to ensure that law enforcement can discover all information subject to seizure pursuant to Section III of Attachment A. Keywords search text, but many common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

Stored Wire and Electronic Communication Access

10. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection -

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant...

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service -

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The government may also obtain records and other information pertaining to a subscriber to or customer of electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(3).

d. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter -
(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

e. Title 18, United States Code, Section 2510, provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .

(17) "electronic storage" means –

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Summary of Investigation and Probable Cause

11. For the reasons set forth below, there is probable cause to believe that evidence of the violation of 18 U.S.C. § 1028 will be located in the records of MICROSOFT relating to the e-mail account [redacted].

12. On June 6, 2008, Library of Congress ("LOC") employees G[redacted] H[redacted] and E[redacted] Y[redacted] filed a complaint with the LOC Office of Inspector General stating that they were victims of identity theft. Further investigation showed that M[redacted] W[redacted], L[redacted] R[redacted], and L[redacted] T[redacted], three additional female LOC employees were also victims of identity theft. All five victims' identities have been compromised at the same companies (Home Depot, Target, Children's Place, and Chase Credit Services, to name a few) where credit accounts had been

opened in their names without their knowledge and information pertaining to their LOC employment was used in the credit application process. I began my investigation by contacting the various stores and credit companies where these LOC employees had reported their identification being compromised. Where possible, I obtained video footage of the instances where any individuals had applied for credit using the personal identifying information of LOC employees.

13. During the course of my investigation, I learned that on May 16, 2008, online credit applications in the names of E[redacted] Y[redacted] and M[redacted] W[redacted] were received by Chase Credit Services and Home Depot over the internet from IP Address 138.88.1.126. Verizon Internet Service provided that on that date IP Address 138.88.1.126 originated and was registered to [redacted].

14. During the course of my investigation, I also obtained video footage from a Target store located at 10500 Campus Way, Largo, Maryland 20774, showing a woman applying for Target credit using E[redacted] Y[redacted]'s identity and purchasing two $300.00 gift cards on May 16, 2008. I then obtained a photograph of [redacted] from the Department of Motor Vehicles ("DMV") in the District of Columbia. That DMV photograph matches the appearance of a person who can be seen in the May 16, 2008 video surveillance footage from Target in Largo, Maryland. That video further shows that while standing at the service counter and working with the same Target cashier, the suspect matching the appearance of [redacted] supplied an additional credit application using LOC employee M[redacted] W[redacted]'s identity. Two

more gift cards in the amount of $300.00 each were subsequently purchased using M[redacted] W[redacted]'s credit.

15. I also obtained video surveillance footage from that same Target store for May 30, 2008. That video shows a suspect matching the appearance of [redacted] applying and receiving Target credit in the names of LOC employees' L[redacted] T[redacted] and L[redacted] R[redacted] while using the same Target cashier from the May 16, 2008 incident at the Largo, Maryland, location.

16. I also obtained video surveillance footage from Home Depot, 6691 Frontier Road, Springfield, Virginia 22150, in connection with an incident that occurred there on May 17, 2008. That video shows a suspect using E[redacted] Y[redacted]'s Home Depot credit to purchase two $2,500 Home Depot gift cards. Based on the DMV photograph that I obtained, the suspect in the May 17, 2008 video from Home Depot appears to be [redacted].

17. On May 18, 2008 a fraudulent Victoria Secret's credit card purchase in the name of E[redacted] Y[redacted] was placed over the internet from IP Address 138.88.1.126, which is registered to [redacted] During my investigation, I learned from United Parcel Service that those items purchased over the internet on May 18, 2008 were delivered on May 21, 2008 to [redacted] home address located at [redacted] The confirmatory email address given by the purchaser for the Victoria Secret website purchase was [redacted].

18. During my investigation I have also learned that on May 27, 2008 and May 30, 2008, credit applications in the names of G[redacted] H[redacted] and L[redacted] R[redacted] were received by GAP Credit Services and Home Depot over the internet from IP Address 141.156.187.214. Verizon Internet Service provided that on these dates the IP Address 141.156.187.214 originated

and was registered to [redacted].

19. As explained above, the e-mail account [redacted] was used as the e-mail account of record in the fraudulent applications for credit applications in the names of E[redacted] Y[redacted] and M[redacted] W[redacted] to Chase Credit Services and Home Depot. That same e-mail address was also used as the purchaser's e-mail address for the fraudulent purchases made in the name of E[redacted] Y[redacted] from the Victoria's Secret website. In my experience, when a person makes an on-line retail transaction a confirmation message is typically sent to the purchaser's e-mail account of record. Thus, it is reasonable to believe that additional e-mail messages referencing those transactions may still exist in that account or in the records of MICROSOFT.

20. A preservation letter pursuant to 18 U.S.C. § 2703(f) was sent to MICROSOFT on July 9, 2008, for the e-mail account [redacted].

21. During my investigation, I have learned from MICROSOFT that this account was created prior to July 9, 2008. Thus, it is reasonable to believe that many e-mails not deleted by the subscriber still exist in those accounts.

Conclusion

22. Based upon the information above, I have probable cause to believe that on the computer systems owned, maintained, and/or operated by Microsoft Corporation there exists evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information). By this affidavit and application, I request that the Court issue a search warrant directed to Microsoft allowing agents to seize the e-mail and other information stored on the Microsoft servers for the computer accounts and files and following the search procedure described in Attachment A.

SPECIAL AGENT DONYA JACKSON
LIBRARY OF CONGRESS
OFFICE OF THE INSPECTOR GENERAL

Sworn and subscribed before me
this ___ day of July 2008

THE HONORABLE DEBORAH A. ROBINSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

I. Search Procedure

a. The search warrant will be presented to Microsoft personnel who will be directed to isolate those accounts and files described in Section II below;

b. In order to minimize any disruption of computer service to innocent third parties, Microsoft employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;

c. Microsoft employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant; and

d. Law enforcement personnel will thereafter review all information and records received from Yahoo employees to determine the information to be seized by law enforcement personnel specified in Section III of Attachment A.

II. Files and Accounts to be Copied by Microsoft Employees

a. All electronic mail stored and presently contained in, or on behalf of, the following electronic mail addresses and/or individual accounts: [redacted];

b. All existing printouts from original storage of all of the electronic mail described above in Section II (a);

c. All transactional information of all activity of the electronic mail addresses and/or individual accounts described above in Section II(a), including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

d. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above in Section II(a), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records, alternate e-mail address, registration from IP, date ID registered, and account log in records (last known IP addresses), and

e. All records indicating the services available to subscribers of the electronic mail addresses and/or individual accounts described above in Section II(a).

III. Information to be Seized by Law Enforcement Personnel

a. All electronic mail stored and presently contained in, or on behalf of, the following electronic mail addresses and/or individual accounts: [redacted] that contains or relates to:

i. Wire fraud, identity theft, bank fraud or computer fraud;

ii. schemes to defraud victims or to obtain personal identification numbers or information from third persons, including efforts to obtain addresses, phone numbers, passwords, tracking numbers, social security numbers, dates of birth, credit card, bank, or other financial information;

iii. communications between co-conspirators of fraud schemes, including criminal misuse of computers;

iv. evidence of accessing computers without authorization or by fraud, including exceeding authorized computer access;

v. means used by co-conspirators to obtain information from victims;

vi. proceeds from fraud schemes or from a conspiracy, including but not limited to wire transfers or use of third parties to send, receive, or hold assets, including money;

vii. identification or associations of co-conspirators, their whereabouts, their role in a conspiracy, or the manner and means of co-conspirators to further the goals and means of the conspiracy.

viii. user attribution evidence, such as an e-mail messages that might indicate the identity of the person sending and receiving e-mail messages as part of a criminal scheme.

b. All existing printouts from original storage of all of the electronic mail described above in Section II (a) of the following electronic mail addresses and/or individual accounts: [redacted] that contains or relates to:

i. Wire fraud, identity theft, bank fraud or computer fraud;

ii. schemes to defraud victims or to obtain personal identification numbers or information from third persons, including efforts to obtain addresses, phone numbers, passwords, tracking numbers, social security numbers, dates of birth, credit card, bank, or other financial information;

iii. communications between co-conspirators of fraud schemes, including criminal misuse of computers;

iv. evidence of accessing computers without authorization or by fraud, including exceeding authorized computer access;

v. means used by co-conspirators to obtain information from victims;

vi. proceeds from fraud schemes or from a conspiracy, including but not limited to wire transfers or use of third parties to send, receive, or hold assets, including money;

vii. identification or associations of co-conspirators, their whereabouts, their role in a conspiracy, or the manner and means of co-conspirators to further the goals and means of the conspiracy.

viii. user attribution evidence, such as an e-mail messages that might indicate the identity of the person sending and receiving e-mail messages as part of a criminal scheme.

c. Any and all electronic file storage associated with [redacted]

Copies of the above-described records and stored information should be obtained from original storage and provided on CD-R (CD-Recordable) media.